

مركز صدور گواهی الكترونيكی پارسساين

راهنمای استفاده از گواهی الکترونیکی در نرمافزار

Microsoft IIS 7

تدوینکنندہ: شرکت امنافزار گستر شریف

SSW_UG_PKI_91109_	شىمارە سىد1
۲۰/مرداد /۱۳۹۲	تاريخ
۱.۸	نگارش

آدرس: تهران، خیابان آزادی، خیابان حبیبالله، خیابان قاسمی غربی، نبش بنبست پیام آزادی، شمارهٔ ۳۷، طبقه پنجم تلفن: ۲۰–۶۱۹۷۵۵۰۱۰ (۲۱) فاکس: ۶۶۰۹۰۲۹۹ (۲۱) سایت اینترنتی: www.parssignca.ir

حق طبع و نشر

این سند در تاریخ ۱۳۹۱/۰۸/۲۴ توسط شرکت امنافزار گستر شریف به منظور تهیه بخشی از اسناد «مرکز صدور گواهی الکترونیکی پارس ساین» تدوین گردیده است. تمامی حقوق این اثر متعلق به «شرکت امنافزار گستر شریف» می باشد و هرگونه نسخه برداری از آن، اعم از کپی، نسخه برداری الکترونیکی و یا ترجمه تمام یا بخشی از آن منوط به کسب اجازه کتبی از صاحب اثر است.

مطالب	فهرست
*	<u> </u>

٩١	مقد	۱
لمیات این سند	فرخ	۲
باد درخواست امضای گواهی (CSR) و کلید خصوصی	ايج	٣
اد فایل گواهی به فرمت PFX	ايج	۴
ربندی IIS به منظور استفاده از گواهی الکترونیکی۶	پيک	۵
نصب گواهي الکترونيکي روي سرور٧	۵–۱	
تخصيص گواهي به وبسايت	۵–۲	
اجباری کردن اتصال HTTPS	۵–۳	
سی صحت نصب گواهی SSL	برر	۶
کلات احتمالی پس از نصب گواهی	مشأ	۷
عدم نمایش قفل کنار عبارت https و عدم نمایش صحیح وبسایت	۱-۷	
نمایش صفحه هشدار SSL در مرورگر	۲-۷	
نمایش صفحه دیگری به جای صفحه سایت	۳-۷	
نمایش صحیح سایت HTTPS در یک مرورگر و عدم نمایش آن در مرورگری دیگر۳۱	۴-۷	
ست	پيو	٨
نحوه بررسی PEM بودن فایل کلید و تبدیل آن به فرمت PEM	۱–۸	
نحوه بررسی PEM بودن فرمت فایل گواهی و تبدیل آن به فرمت PEM	۲–۸	

۱ مقدمه

تأمین امنیت ارتباطات و تبادلات الکترونیکی در شبکهها خصوصاً محیط اینترنت از جمله مسائل ویژهای است که امروزه سازمانها با آن مواجه هستند. به دلیل حساسیت امنیتی حجم قابل توجهی از این تبادلات در محیط وب، باید تدابیر امنیتی لازم در پروتکلها و سرویسهای مورد استفاده در این نوع ارتباطات اتخاذ گردد. پروتکل HTTP (که عموماً به عنوان پروتکل وب شناخته میشود) یکی از این پروتکلها است که استفاده گستردهای دارد. دادههای HTTP به صورت ناامن روی شبکه منتقل میشوند؛ از اینرو، دادههایی که بین سرویسدهنده⁽ (سمت وبسایت) و سرویسگیرنده^۲ (سمت کاربر وبسایت) مبادله میشود، توسط مهاجمین قابل مشاهده و حتی قابل تغییر هستند.

وبسایتهایی که اطلاعات مهم و محرمانه (مانند گذرواژه، شماره کارت اعتباری، اطلاعات بانکی، و دیگر اطلاعات خصوصی) با کاربران مبادله میکنند، نباید از پروتکل ناامن HTTP استفاده نمایند. نسخه امنشده این پروتکل به نام HTTPS، پرکاربردترین پروتکل امنیتی مبتنی بر رمزنگاری کلید عمومی است که در پیادهسازی این گونه وبسایتها به کار میرود. این پروتکل مبتنی بر پروتکل میاند.

لازم به ذکر است، تأمین محرمانگی و عدم تغییر (جامعیت) اطلاعات تبادل شده بین کاربر و وبسایت تنها کاربرد HTTPS نیست. HTTPS برای جلوگیری از حملاتی مانند حمله فیشینگ مبتنی بر جعل سایت نیز استفاده می شود. در حمله مذکور، حمله کننده (مثلاً یک رقیب تجاری) با ایجاد یک وبسایت با ظاهری کاملاً مشابه سایت اصلی، کاربران آن سایت را به سایت جعلی هدایت کرده و امنیت آن ها را به مخاطره می اندازد؛ مثلاً اطلاعات کاربران را به سرقت می برد یا در مورد آن ها اطلاعات جمع آوری می کند. در صورتی که از گواهی HTTPS استفاده شود، از این حمله جلوگیری می شود.

در پیکربندی وب سرور برای استفاده از HTTPS، از یک گواهی الکترونیکی SSL استفاده می شود. این گواهی باید توسط یک مرکز صدور گواهی الکترونیکی معتبر (مانند مرکز صدور گواهی الکترونیکی پارس ساین) صادر شده باشد تا کاربران بتوانند به آن اعتماد کرده و اطلاعات محرمانه خود را بر اساس این اعتماد، برای وب سایت ارسال نمایند.

© Copyright Amnafzar Co.

¹ Server

² Client

۲ فرضیات این سند

در این سند، نحوه استفاده از گواهی الکترونیکی، بر اساس سناریوی فرضی زیر در نظر گرفته شده است: «برای یک وبسایت به آدرس www.mydomain.com، میخواهیم از مرکز صدور گواهی الکترونیکی پارسساین، گواهی SSL درخواست نماییم. پس از دریافت گواهی، فایل گواهی به فرمت PFX را ایجاد نموده و آن را در نرمافزار Microsoft IIS 7 به وبسایت مورد نظر تخصیص دهیم. سپس وب سرور را طوری تنظیم نماییم که امکان برقراری ارتباط HTTPS با آن فراهم شود».

از اینرو، به منظور استفاده از این سند در سناریوی واقعی، باید به موارد زیر دقت نمایید:

- به جای آدرس www.mydomain.com، باید از آدرس دقیق وبسایتی استفاده نمایید که برای آن
 گواهی SSL درخواست نمودهاید.
- در مثال فرضی ما، وبسایت پیشفرض (Default Web Site) در وبسرور IIS، سایت
 سایت همیشه این گونه نباشد، باید مراحل گفته شده در این سند را برای سایت مورد نظر خود انجام دهید.

۳ ایجاد درخواست امضای گواهی (CSR) و کلید خصوصی

برای دریافت گواهی الکترونیکی از مرکز صدور گواهی الکترونیکی پارس ساین، ابتدا باید یک درخواست امضای گواهی (CSR) ایجاد نماییم. لازم به ذکر است که فیلدهای CSR باید طبق سیاست های مرکز صدور گواهی پارس ساین تکمیل گردد. در غیر این صورت، مرکز پارس ساین برای آن CSR، گواهی الکترونیکی صادر نخواهد کرد.

در نرمافزار IIS، فرایند ایجاد CSR و تکمیل فیلدهای آن با «سند جامع پروفایل های زیرساخت کلید عمومی کشور» تطابق ندارد. از اینرو توصیه می شود برای ایجاد CSR از نرمافزار به بخش دانلود سایت مرکز به شرکت امنافزار گستر شریف استفاده نمایید. برای دریافت این نرمافزار به بخش دانلود سایت مرکز صدور گواهی الکترونیکی پارس ساین به آدرس /parskey Utility مراجعه کنید. همچنین، سند "راهنمای ایجاد CSR با استفاده از نرمافزار vility و Parskey Utility" در بخش راهنماها از سایت مذکور قابل دانلود است. نحوه ایجاد CSR برای گواهی SSL، در بخش "پروفایل گواهی SSL" از سند مذکور تشریح شده است.

پس از ایجاد CSR و کلید خصوصی (این کلید هنگام ایجاد CSR تولید می گردد)، فایل CSR باید به مرکز صدور گواهی الکترونیکی پارسساین تحویل داده شود تا گواهی SSL متناظر آن را صادر نماید. دقت نمایید برای صدور گواهی توسط مرکز پارسساین، تنها به فایل CSR نیاز می باشد و نباید فایل کلید خصوصی به این مرکز تحویل داده شود.

هشدار: سرور از فایل کلید خصوصی برای رمزگذاری و رمزگشایی دادهها استفاده مینماید. از اینرو، در محافظت از کلید خصوصی دقت نمایید. در صورتی که این کلید در دسترس افراد غیرمجاز قرار گیرد، کلیه دادههای رمزشده بین وبسایت و کاربران میتواند توسط این افراد رمزگشایی شود.

۴ ایجاد فایل گواهی به فرمت PFX

پس از دریافت گواهی الکترونیکی SSL از مرکز پارسساین، باید آن را به فایلی با فرمت PFX تبدیل نماییم که شامل گواهی SSL صادرشده و کلید خصوصی متناظر آن میباشد. ابتدا باید از PEM بودن

© Copyright Amnafzar Co.

¹ Certificate Signing Request (CSR)

فرمت فایل های گواهی و فایل کلید خصوصی اطمینان حاصل نماییم. لازم به ذکر است، در صورتی که CSR با نرمافزار ParsKey Utility تولید شده باشد، فایل کلید خصوصی در فرمت PEM میباشد. نحوه بررسی PEM بودن فایل کلید خصوصی در بخش ۸–۱ از پیوست تشریح شده است. همچنین، نحوه بررسی PEM بودن فایل گواهی، در بخش ۸–۲ از پیوست آمده است. برای ایجاد این فایل مراحل زیر را انجام میدهیم:

 ۱. نرمافزار OpenSSL را از بخش دانلود وبسایت مرکز صدور گواهی الکترونیکی پارسساین به آدرس www.parssignca.ir دریافت و روی سیستم خود نصب مینماییم.

 ۲. اگر نسخهی تحت ویندوز OpenSSL را نصب کرده باشیم، به دایرکتوری bin در مسیر نصب نرمافزار رفته (این مسیر در ویندوز 7 نسخه ۶۴ بیتی، C:\OpenSSL-Win64\bin میباشد) و فایل اجرایی OpenSSL به نام openssl.exe را اجرا مینماییم. با اجرای این برنامه، پنجرهای مانند شکل زیر ظاهر

	می گردد.
C:\OpenSSL-Win64\bin\openssl.exe	
OpenSSL>	

۳. روبروی عبارت <OpenSSL در پنجره فوق، دستور زیر را وارد می نماییم:

pkcs12 -export -out mydomain.pfx -inkey key.pem -in mydomain.cer لازم به ذكر است كه اگر با لينوكس كار مىكنيم، فرمان زير را به جاى دستور فوق بايد وارد نماييم:

openssl pkcs12 -export -out mydomain.pfx -inkey key.pem -in mydomain.cer

در دستور فوق:

- key.pem، فایل کلید خصوصی با فرمت PEM میباشد؛
 - mydomain.cer فایل گواهی با فرمت PEM میباشد؛
- mydomain.pfx فایل خروجی ایجاد شده با فرمت PEM می باشد.

با وارد نمودن دستور فوق، از ما خواسته می شود گذرواژه کلید خصوصی (که هنگام ایجاد CSR تعیین نمودهایم) را وارد نماییم. در مرحله بعد، از ما خواسته می شود گذرواژه فایل PFX را وارد نماییم، که باید گذرواژهای را وارد نماییم تا فایل PFX ایجاد گردد. دقت کنید، هنگام تایپ این گذرواژهها، کاراکترهای

این ترتیب، دستور به صورت زیر خواهد بود:

آنها در صفحه نمایش داده نمیشود و مکاننما حرکت نمیکند؛ شما بدون توجه به این مسأله گذرواژه را

لازم به ذکر است در دستور فوق، باید برای هر یک از فایل ها، مسیر دقیق آنها را وارد نماییم. برای مثال،

در صورتی که فایل های key.pem و mydomain.cer، و را در پوشهی certs از درایو D قرار داده باشیم و

pkcs12 -export -out d:\certs\mydomain.pfx -inkey d:\certs\key.pem

در صورت استفاده از لینوکس، فرض میکنیم فایلهای مذکور در مسیر home/certs/ قرار داشته باشند. به

بخواهیم فایل mydomain.pfx نیز در همین مسیر ذخیره گردد، دستور به صورت زیر خواهد بود:

وارد کنید). گذرواژه را به خاطر بسپارید زیرا هنگام نصب گواهی باید آن را وارد نمایید.

openssl pkcs12 -export -out /home/certs/mydomain.pfx -inkey

/home/certs/key.pem -in /home/certs/mydomain.cer

-in d:\certs\mydomain.cer

۵ پیکربندی IIS به منظور استفاده از گواهی الکترونیکی

پس از ایجاد فایل PFX گواهی SSL (طبق بخش ۴)، می توانیم تنظیمات لازم را در نرمافزار IIS 7 به ترتیب زیر انجام دهیم:

- د نصب گواهی الکترونیکی به فرمت PFX روی سرور؛
 - ۲. تخصیص گواهی به وبسایت مورد نظر در IIS؛
- ۳. تنظیم وبسرور برای اجباری نمودن استفاده از پروتکل HTTPS.

در بخشهای بعد، هر یک از مراحل فوق با جزییات تشریح میگردد.

۱–۵ نصب گواهی الکترونیکی روی سرور

پس از ایجاد فایل گواهی به فرمت PFX مطابق بخش ۴، فایل گواهی PFX را روی سروری که برای آن گواهی SSL صادر شده است، نصب مینماییم. رویه این کار به صورت زیر میباشد:

۳. در منوی Start، عبارت mmc را در جعبه search programs and files وارد مینماییم تا برنامه mmc . در لیست Programs ظاهر گردد، روی آن کلیک میکنیم (شکل زیر).



۲. در کنسول بازشده، در سربرگ File روی گزینه Add/Remove Snap-in کلیک می نماییم (شکل زیر).

1	Console1 nsole	Root]					
	File Acture View	Favorites	Window	Help			_ 8 ×
	New		Ctrl+N				
	Open Save	_	Ctrl+O Ctrl+S			Actions	
	Save As	2		There are no ite	ms to show in this view.	Console Root	-
	Add/Remove Snap-in	т <u>,</u>	Ctrl+M			More Actions	•
	Options						
	1 C: \Users \ \Deskt	top\Console 1	L				
	2 ServerManager			_			
	Exit						
Ι.							

۲. در پنجره Add or Remove Snap-ins، گزینه Certificates را انتخاب نموده (مرحله ۱ از شکل زیر) و

سپس روی Add کلیک مینماییم (مرحله ۲ از شکل زیر).

nap-in	Vendor		[Console Root	Edit Extensions
ActiveX Control	Microsoft Cor				-
Authorization Ma	Microsoft Cor				Remove
Certificates	Microsoft Cor				
Component Services	Microsoft Cor		2		Move Up
Computer Managem	Microsoft Cor		~		
Device Manager	Microsoft Cor				Move Down
Disk Management	Microsoft and		Add >		
Event Viewer	Microsoft Cor		\smile		
Folder	Microsoft Cor				
Group Policy Object	Microsoft Cor				
Internet Information	Microsoft Cor				
Internet Information	Microsoft Cor				
IP Security Monitor	Microsoft Cor				
IP Security Policy Ma	Microsoft Cor	•			Advanced
ription:					
IP Security Policy Ma	Microsoft Cor	<u> </u>	L		

۴. در پنجره Certificates snap-in، گزینه Computer account را انتخاب نموده و روی Next کلیک مینماییم (شکل زیر).

C	Certificates snap-in	×
	This snap-in will always manage certificates for:	
	O My user account O Service account	
	2	
	< Back Next > Cancel	

۵. در پنجره Select Computer، گزینه Local computer به صورت پیش فرض انتخاب شده می باشد.
 ۹. بدون تغییر آن روی Finish کلیک می نماییم (شکل زیر).

Select Computer		x
This snap-in will always ma	nt this snap-in to manage. nage: computer this console is running on)	
C Another computer:	Browse	
Allow the selected co only applies if you sav	mputer to be changed when launching from the command line. This re the console.	
		J
	2	
	< Back Finish Cancel	

۶. در پنجره Add or Remove Snap-ins، روی OK کلیک مینماییم (شکل زیر).

ActiveX Control Microsoft Cor Authorization Manager Microsoft Cor Certificates Microsoft Cor Component Services Microsoft Cor Device Manager Microsoft Cor Device Manager Microsoft Cor Disk Management Microsoft Cor Folder Microsoft Cor Group Policy Object Microsoft Cor Internet Information Microsoft Cor IP Security Monitor Microsoft Cor	European Eur	dit Extensions.
Computer Managem Microsoft Cor Device Manager Microsoft Cor Disk Management Microsoft Cor Event Viewer Microsoft Cor Folder Microsoft Cor Group Policy Object Microsoft Cor Internet Information Microsoft Cor Internet Information Microsoft Cor IP Security Monitor Microsoft Cor	oft Cor Certificates (Local Computer) oft Cor oft Cor	Remove Move Up
IP Security Monitor Microsoft Cor	Add > 5ft cor oft cor oft Cor oft Cor oft Cor oft Cor	Move Down
IP Security Policy Ma., Microsoft Cor.,	oft Cor A	Advanced

۷. در منوی وسط، روی (Certificates (Local Computer دو بار کلیک مینماییم (شکل زیر).

🚟 File Action View Favorites Window Help		_ 8 ×
Console Root Name	Actions	
🗉 🗐 Certificates (Local Com	Console Root	-
	More Actions	►

۸ در بخش Logical Store Name، روی Personal کلیک راست نموده، گزینه All Tasks (مرحله ۱ از شکل زیر) و سپس Import را انتخاب مینماییم (مرحله ۲ از شکل زیر).

Logical Store Name	
Pers Find Certificates	Find Certificates Request New Concern Import Advanced Operations
Trusted Devices	



۹. در پنجره Certificate Import Wizard، روی Next کلیک می نماییم (شکل زیر).

۱۰. با کلیک روی Browse، فایل گواهی با فرمت PFX را انتخاب نموده و سپس روی Next کلیک مینماییم.

Certificate Import Wizard	X
File to Import	
Specify the file you want to import.	
File name:	
Browse	
Note: More than one certificate can be stored in a single file in the following formats:	
Personal Information Exchange - PKCS #12 (.PFX,.P12)	
Cryptographic Message Syntax Standard-PKCS #7 Certificates (.P7B)	
Microsoft Serialized Certificate Store (.SST)	
Learn more about <u>certificate file formats</u>	
< Back Next > Cance	el 🛛

۱۱. فرمت فایل را از نوع (Personal Information Exchange (*.pfx;*.p12 قرار داده (مرحله ۱ از شکل زیر)، سپس فایل pfx را در مسیر ذخیره آن انتخاب نموده (مرحله ۲ از شکل زیر) و روی دکمه Open کلیک مینماییم.

🚟 Open				×	-
Comp	uter 🔻 Local Disk (C:) 👻	👻 🛃 Se	arch Local Disk (C:)	1	ns
Organize 🔻 New folde	r				onal
Downloads	▲ Name ^		Date modified	Туре	lore A
🔚 Recent Places	\mu inetpub		9/17/2012 10:56 AM	File folder	
🔚 Libraries	PerfLogs		7/14/2009 7:50 AM	File folder	
Documents	🐌 Program Files		9/17/2012 10:56 AM	File folder	
J Music	Program Files (x86)		9/17/2012 10:56 AM	File folder	L
Pictures	Users		9/17/2012 10:57 AM	File folder	L
💾 Videos	Windows 2		11/7/2012 10:59 AM	File folder	
Computer	mydomain		11/7/2012 9:30 AM	Personal Info	
Network	•			Þ	
E		- ¥5	i00 Certificate (* cerv* /	-r+) v	
			09 Certificate (*.cer.*.c	-rt)	Ŀ
		Per Per	sonal Information Exc	hange (*.pfx;*	.p12)
		Ce	rtificate Trust List (*.st	l) -+ (*1)	
P	•	Mi	crosoft Serialized Certi	ficate Store (*	.sst)
	,	РК	CS #7 Certificates (*.sp	oc;*.p7b)	,
		All	Files (*.*)		

۱۲. پس از وارد نمودن فایل گواهی با فرمت PFX، روی Next کلیک مینماییم (شکل زیر).

Certificate Import Wizard	×
File to Import	
Specify the file you want to import.	
File name:	
C:\mydomain.pfx Br	owse
Note: More than one certificate can be stored in a single file in the following	g formats:
Personal Information Exchange- PKCS #12 (.PFX,.P12)	
Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)	
Microsoft Serialized Certificate Store (.SST)	
Learn more about <u>certificate file formats</u>	
< Back Next >	Cancel

۱۳. گذرواژهای که هنگام ایجاد فایل pfx تعیین نمودهایم را وارد می نماییم (مرحله ۱ از شکل زیر). در صورت تمایل، می توانید گزینه "...Mark this key as exportable" را انتخاب نمایید. گزینه "Include all extended properties" به صورت پیش فرض انتخاب شده است (مرحله ۲ از شکل زیر)، بدون تغییر آن روی Next کلیک می نماییم (مرحله ۳ از شکل زیر).

نکته: با انتخاب گزینه ".... pfx می توانیم فایل mark this key as exportable"، به منظور انتقال فایل pfx به سرور دیگر یا تهیه نسخه پشتیبان از آن، می توانیم فایل pfx را استخراج نماییم. در صورتی که به دلیل حساسیت امنیتی نخواهید کلید خصوصی از روی سرور قابل استخراج باشد، این گزینه را انتخاب نکنید (آن را تیک نزنید).



۱۴. گزینه "Automatically select the certificate store based on the type of certificate" را انتخاب

نموده و روی Next کلیک مینماییم (شکل زیر).

Certificate Import Wizard	×
Certificate Store	
Certificate stores are system areas where certificates are kept.	
	_
Windows can automatically select a certificate store, or you can specify a location for the certificate.	
Automatically select the certificate store based on the type of certificate	
O Place all certificates in the following store	
Certificate store:	
Personal Browse,	
Learn more about <u>certificate stores</u>	
2	
< Back Next Cancel	

۱۵. پیغامی مبنی بر موفق بودن نصب گواهی ظاهر میگردد. روی OK کلیک مینماییم (شکل زیر). در پایان پنجره کنسول را میبندیم. لازم به ذکر است نیازی به ذخیره کردن کنسول نمیباشد.

Certificate	e Import Wizard	×
i	The import was successful.	
	OK	

۲-۵ تخصیص گواهی به وبسایت

پس از نصب گواهی روی سرور، باید در نرمافزار IIS آن را به وبسایت مورد نظر تخصیص دهیم. رویه این کار به صورت زیر میباشد:

۰. در منوی Start، در بخش Administrative Tools، روی ا. در منوی Internet Information Services (IIS) Manager

		🕌 Remote Desktop Services 🔹 🕨
		Component Services
		😓 Computer Management
		🔄 Data Sources (ODBC)
		Event Viewer
		1 Internet Information Services (IIS) 5.0 Manager
Manager	(C)-m	Internet Information Services (IIS) Manager
	∛ ∭∭≣∣	😪 iSCSI Initiator
Internet Explorer		Local Security Policy
	user	N Performance Monitor
		here a security Configuration Wizard
Command Prompt	Documents	🚠 Server Manager
Command Prompt		Services
	Computer	📆 Share and Storage Management
	Network	🕎 Storage Explorer
		System Configuration
	Control Panel	Task Scheduler
		Windows Firewall with Advanced Security
2	Devices and Printers	Windows Memory Diagnostic
	Administrative Tools	Windows PowerShell Modules
	Administrative roots	Windows Server Backup
	Help and Support	
	Run	
All Programs		
Search are and flee	Log off	
🎝 Start 👢 ⊿ 🚞		

۲. در منوی Connections روی نام سرور مورد نظر کلیک مینماییم (مرحله ۱ از شکل زیر). در لیست
 ۲. در منوی Connections روی گزینه (در مرحله ۲ از شکل زیر). در منوی Actions، روی گزینه Sites
 ۲. سایت مورد نظر را انتخاب میکنیم (در مرحله ۲ از شکل زیر). در منوی Bindings

¥ Internet Information Services (115) Manag	er	
O NIN-JBVDDKCBCQ7 ► Site	s 🕨 www.mydomain.com 🕨) 🖾 🖂 🔐 -
File View Help		
Connections Start Page WIN-JBVDDKCBCQ7 (WIN-JBVDDKCBCQ7Y Application Pools Stes Www.mydomain.com	WWW.mydomain.com Home Filter: Image: Show All Group by: ASP.NET Image: Show All Group by: Asp.net Image: Show All Group by: Asp.net Image: Show All Group by: Image: Asp.net Image: Show All Group by: Image: Show All Group by: Image: Asp.net Image: Show All Group by: Image: Show All Group by: Image: Show All Group by: Image: Asp.net Image: Show All Group by: Image: Asp.net Image: Show All Group by: Image: Asp.net Image: Show All Group by: Image: Show All Group by: Image: Show All Group by:	Actions Explore Edit Permissions Edit Site Bindings Basic Settings View Applications View Virtual Directories Manage Web Site Restart Start Start Stop Browse Web Site Browse *:80 (http) Browse *:80 (http) Browse *:80 (http) Browse *:443 (https) Advanced Settings Configure Failed Request Tracing Limits Add FTP Publishing \widehat{C} Help Online Help

۳. در پنجره بازشده (شکل زیر)، روی دکمه Add کلیک مینماییم.

Si	te Bindin	gs				? ×
	Type http	Host Name	Port 80	IP Address *	Binding	Add
						Remove
	•					Browse
						Close

۴. در پنجره بازشده (شکل زیر)، تنظیمات زیر را انجام میدهیم:

- از لیست Type، گزینه HTTPS را انتخاب می کنیم (مرحله ۱ از شکل زیر).
- از لیست IP Address، آدرس IP سایت را را انتخاب می کنیم (مرحله ۲ از شکل زیر).
 از لیست IP Address، برای استفاده از HTTPS برای یک دامنه (وبسایت)، باید یک آدرس IP نکته بسیار مهم: برای استفاده از آدرس نباید با دامنه های دیگر به اشتراک گذاشته شود.
 در غیر اینصورت، امکان استفاده از HTTPS وجود نخواهد داشت.
- از لیست Port، شماره درگاه 443 (شماره درگاه پیشفرض) را انتخاب میکنیم (مرحله ۳ از شکل زیر). در صورت تمایل، می توانیم شماره درگاه دیگری را نیز وارد کنیم. در این صورت، دسترسی به سایت از طریق HTTPS باید با استفاده از این شماره درگاه انجام شود. از اینرو، کاربران وبسایت باید از این شماره درگاه مطلع شوند.
- از لیست SSL Certificate، گواهی مربوط به وبسایت را مطابق مرحله ۴ از شکل زیر انتخاب میکنیم (این گواهی قبلاً طبق بخش ۵–۱ روی سرور نصب شده است).

در پایان، روی دکمه OK کلیک مینماییم (شکل زیر).

Add Site Binding	<u>?</u> ×
Type: 1 IP address: https 5.254.242.180	2 Port: 3
Host name:	
J SSL certificate:	- 4
www.mydomain.com	View
5.	OK Cancel

¹ Dedicated IP Address

۵. در پنجره زیر، روی دکمه Close کلیک مینماییم.

S	ite Bindin	igs				?×
	Type http https	Host Name	Port 80 443	IP Address * 65.254.242.180	Binding	Add Edit
						Remove
						Browse
	•				Þ	
						Close

پس از این مرحله، گواهی HTTPS به وبسایت تخصیص داده شده است و با استفاده از HTTPS می توان به سایت دسترسی داشت با این وجود، در برخی موارد باید IIS راهاندازی مجدد شود تا بتوان از سرویس HTTPS استفاده نمود. لازم به ذکر است که در این مرحله با استفاده از HTTP نیز می توان به سایت دسترسی داشت؛ به منظور برقراری ارتباط تنها از طریق HTTPS، باید طبق بخش ۵–۳ عمل نماییم.

¹ Restart

© Copyright Amnafzar Co.

HTTPS اجباری کردن اتصال HTTPS

برای آنکه اتصال به سایت مورد نظر تنها به صورت HTTPS قابل انجام باشد، باید تنظیمات لازم در نرمافزار IIS انجام شود. در غیر این صورت، کاربران در صورت تمایل می توانند با پروتکل ناامن HTTP به سایت متصل شوند و در نتیجه در معرض مخاطرات امنیتی مختلفی قرار گیرند. برای اجباری نمودن برقراری ارتباط HTTPS به سایت، به صورت زیر عمل می نماییم:

۱. در منوی Start، در بخش Administrative Tools روی (IIS) . در منوی Manager کلیک مینماییم (شکل زیر).

		🕌 Remote Desktop Services 🔹 🕨
		🚱 Component Services
		😓 Computer Management
		Data Sources (ODBC)
		Event Viewer
	eQ.5	Internet Information Services (IIS) 6.0 manager
Manager		Internet Information Services (IIS) Manager
	<u> </u>	😪 iSCSI Initiator
Internet Explorer	~ <u>~</u>	🚡 Local Security Policy
	user	N Performance Monitor
Notepad •		a Security Configuration Wizard
	Documents	Server Manager
Command Prompt		Services
	Computer	Share and Storage Management
		Storage Explorer
	Network	System Configuration
	Control Banal	Task Scheduler
	Control Panel	Windows Firewall with Advanced Security
	Devices and Printers	Windows Memory Diagnostic
		🔀 Windows PowerShell Modules
	Administrative Tools 🔹 🕨	Windows Server Backup
	Hele and Concert	
	help and support	
	Run	
All Programs		
Search pro 1 and files	Log off	
🔊 Start 🏭 🗾 🚞		

۲. در منوی Connections روی نام سرور مورد نظر کلیک مینماییم (مرحله ۱ از شکل زیر). در لیست Sites، سایت مورد نظر را انتخاب میکنیم (مرحله ۲ از شکل زیر). در منوی وسط روی SSL Settings دابلکلیک مینماییم (مرحله ۳ از شکل زیر).



۳. در پنجره بازشده (شکل زیر)، گزینه Require SSL را انتخاب میکنیم (مرحله ۱ از شکل زیر). در بخش Client certificates نیز میتوانیم بسته به سیاستهای وبسایت خود در دسترسی سرویس گیرندگان، گزینه مناسب را انتخاب نماییم؛ گزینه پیشفرض، گزینه Ignore میباشد. در پایان، در منوی Actions روی Apply کلیک مینماییم (مرحله ۲ از شکل زیر). در صورت موفق. ودن اِعمال تغییرات، در منوی The changes have been successfully applied نمایش داده میشود.



۶ بررسی صحت نصب گواهی SSL

برای برقراری ارتباط صحیح SSL میان مرورگر کاربر و وبسایت، کاربر وبسایت باید زنجیره گواهی را روی سیستم یا مرورگر خود نصب نماید. رویه این کار در سند «راهنمای نصب زنجیره گواهی» تشریح شده است. این سند را میتوانید از بخش "راهنماها" در وبسایت مرکز پارسساین به آدرس www.parssignca.ir دانلود و مطالعه نمایید. پس از نصب صحیح زنجیره گواهی، در نوار آدرس مرورگر، آدرس https://www.mydomain.com باید آدرس دقیق سایت خود را وارد نمایید). نمایش علامت قفل به همراه عبارت https در نوار آدرس مرورگرها یکی از نشانههای صحیح بودن نصب گواهی SSL در وبسایت میباشد. نمایش علامت قفل در سه مرورگر Internet Explorer، Google Chrome به صورت زیر میباشد:

 مرور گر Google Chrome: در نوار آدرس (مطابق شکل زیر) قفل سبز رنگ در کنار عبارت سبز رنگ https ظاهر می شود.



برای اطمینان کامل از صحت نصب گواهی، در مرورگر خود روی علامت قفل کلیک نموده و روی لینک Internet Explorer در View Certificates، Google Chrome در Certificate Information و More Information در Firefox کلیک نمایید. سپس اطمینان حاصل کنید که گواهی نشانداده شده، همان گواهی است که مرکز پارس ساین برای وب سایت شما صادر نموده است.

- ۷ مشکلات احتمالی پس از نصب گواهی
- ۱–۷ عدم نمایش قفل کنار عبارت https و عدم نمایش صحیح وبسایت

در صورتی که نصب گواهی روی سرور، همچنین نصب زنجیره روی مرورگر، هر دو به درستی انجام شده باشند اما در مرورگرها شکلهای زیر نمایش داده شود:

 مرور گر Google Chrome: در نوار آدرس مرور گر، علامت مثلث روی قفل کنار https نشان داده شود (مانند شکل زیر).

/ mydomain	×
$\leftrightarrow \ \Rightarrow \ C$	https://www.mydomain.com

• مرورگر Firefox: در نوار آدرس مرورگر، علامت قفل کنار https ظاهر نشود (مانند شکل زیر).

+ Chttps://	ww.mydomain.com
	This website does not supply identity information.
	Your connection to this site is only partially encrypted, and does not prevent eavesdropping. More Information

• مرورگر Intenet Explorer: در پایین صفحه، پیامی مانند شکل زیر ظاهر گردد.



• مرور گر Opera: در نوار آدرس مرور گر، علامت Secure کنار https ظاهر نشود (مانند شکل زیر).

← → ⊃ ⊶ 🔇 https://www.mydomain.com/

• مرورگر Safari: در انتهای نوار آدرس مرورگر، علامت قفل ظاهر نشود (مانند شکل زیر).

+ 🔄 https://www.mydomain.com/

این مشکل معمولاً Mixed content warning نامیده می شود که ممکن است یک حمله کننده با استفاده از آن امنیت کاربران سایت شما را به مخاطره اندازد. این مشکل مربوط به گواهی SSL

¢

سایت نیست، بلکه به کد وبسایت یا تنظیمات سرور شما مربوط میباشد. دلیل مشکل این دلیل است که در وبسایت شما از محتوای ناامن استفاده شده است. مثالهایی از محتوای ناامن، عکسها، اسکریپتها، یا CSSهایی هستند که به طور ناامن (از طریق HTTP) در سایت شما بارگذاری میشوند. مرورگر از بارگذاری یا اجرای این محتواها جلوگیری میکند. به همین دلیل ممکن است CSS وبسایت شما بارگذاری نشده و ساختار وبسایت شما با HTTP به هم بریزد، عکسی بارگذاری نشود، یا اسکریپتی اجرا نشود. برای کشف محتوای ناامن، میتوانید از قابلیت Tob Developer Toolbar در اغلب مرورگرها

استفاده کنید. کشف محتوای ناامن با استفاده از مرورگرهای رایج معمولاً به صورت زیر میباشد:

- مرور گر Google Chrome و Internet Explorer: فشردن کلید F12 و مشاهده خطاها در بخش Console.
- مرور گر Firefox: فشردن کلیدهای Ctrl + Shift + K و مشاهده خطاهای Mixed Content. پس از کشف محتوای ناامن، آنها را از طریق HTTPS بارگذاری نموده و در صورت عدم امکان بارگذاری با استفاده از HTTPS، آنها را از وبسایت خود حذف نمایید. در زیر چند سناریو از محتوای ناامن توصیف شده است.
- CSS فرض صورت به سايت کنىد مثال، • برای http://www.mydomain.com/templates/mystyle.css در صفحه سایت فراخوانی شده باشد. در این صورت، به دلیل استفاده از http (به جای https) این محتوا توسط مرورگر ناامن تشخیص داده شده و بارگذاری نمی شود (در نتیجه ساختار سایت بهم میریزد). بنابراین توصیه می شود به جای استفاده از آدرس.های ثابت (hard-coded) برای عکس.ها، CSS، و اسکرییت.های سایت، از روشهایی مانند آدرسهای نسبی، توابع (مثلاً ()include)، یا هر روش دیگری استفاده نمایید که با استفاده از آن بتوان محتوا را با استفاده از https بارگذاری نمود. در صورتی که از روشی مانند آدرس دهی نسبی استفاده کنید اما مشکل همچنان باقی باشد، مشکل مربوط به تنظیمات SSL در سرور شما ميباشد.
- در برخی موارد، ممکن است آدرس عکس، CSS، یا اسکریپت با https باشد اما مرورگر آن را بارگذاری نکند. این مشکل معمولاً به این دلیل است که مثلاً CSS با آدرس

¹ Content

© Copyright Amnafzar Co.

ما (www) فراخوانی شده است اما (ttps://mydomain.com/templates/mycss.css) فراخوانی شده است اما آدرس درج شده در گواهی سایت، با www است. در این مثال، راه حل این است آدرس https به طور دقیق و طبق آنچه در گواهی SSL سایت درجشده وارد شود.

- مثال دیگر از محتوای ناامن، استفاده از اسکرپیتهایی است که با استفاده از http اطلاعاتی را از سایت ما برای سایت دیگری (مثلاً برای یک سایت ثبت آمار کاربران) ارسال میکنند. همچنین، اسکرپیتها، عکسها، و غیره که از سایت دیگر به صورت http در سایت ما بارگذاری میشوند. مرورگر از بارگذاری و اجرای این محتواها نیز جلوگیری میکند. در صورتی که امکان بارگذاری این مرورگر از بارگذاری و اجرای این محتواها نیز جلوگیری میکند. در صورتی که امکان بارگذاری این مرورگر این مید. در صورتی که امکان بارگذاری این مرورگر از بارگذاری و اجرای این محتواها نیز جلوگیری میکند. در صورتی که امکان بارگذاری این مرورگر از بارگذاری و اجرای این محتواها نیز جلوگیری میکند. در صورتی که امکان بارگذاری این مرورگر این محتواها از طریق http وجود ندارد، آنها از وبسایت خود حذف نمایید. روش دیگر این است که دو صفحه مجزا، یکی برای http و یکی برای https محتوای ناامن را حذف کنید. سپس است که دو صفحه مجزا، یکی برای SSL را به آدرس صفحه وای ناامن را حذف کنید. سپس در تنظیمات SSL روی سرور، درخواستهای SSL را به آدرس صفحه محتوای زا از سایت مذکور در دیگر این است که به جای دریافت محتوا (مثلاً عکس) از سایت دیگر، محتوا را از سایت مذکور در دیگر این در یافت محتوای زامن را حفود مدور، درخواستهای SSL را به آدرس صفحه زا، یکی برای و SSL را به آدرس صفحه و محتوای زامن را حذف کنید. سپس در مذکور در تنظیمات SSL روی سرور، درخواستهای SSL را به آدرس صفحه زا از سایت مذکور در دیگر این است که به جای دریافت محتوا (مثلاً عکس) از سایت دیگر، محتوا را از سایت مذکور در یافت و در منابع سایت خود قرار دهید. سپس به طور محلی آنها را فراخوانی/بارگذاری کنید.
- در برخی موارد، ممکن است محتوا از سایت دیگر و با https فراخوانی شود، اما توسط مرورگر بارگذاری نشود. این مشکل معمولاً دلایل مختلفی میتواند داشته باشد که همگی بستگی به سرویس HTTPS سایت ارسالکننده محتوا دارد. مثلاً ممکن است گواهی SSL آن سایت، برای مرورگر مورد اعتماد نباشد. برای حل این مشکل، وضعیت سرویس HTTPS سایت ارسالکننده را بررسی نمایید.

۲–۷ نمایش صفحه هشدار SSL در مرورگر

در حالت کلی این گونه هشدارها را به دقت مطالعه نموده و دلیل آن را بررسی نمایید.

در صورتی که نصب گواهی روی سرور، همچنین نصب زنجیره روی مرورگر، هر دو به درستی انجام شده باشند اما در مرورگرها شکلهای زیر نمایش داده شود:

• مرور گر Google Chrome: پیام زیر نمایش داده شود.



• مرور گر Firefox پیام زیر نمایش داده شود.

	This Connection is Untrusted
	You have asked Firefox to connect securely mydomain.com but we can't confirm that your connection is secure.
	Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.
	What Should I Do?
	If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.
	Get me out of here!
,	Technical Details
	parssignca.ir uses an invalid security certificate.
	The certificate is only valid for <u>www.mydomain.c</u> om
	(Error code: ssl_error_bad_cert_domain)
	L Understand the Picks

• مرور گر Internet Explorer: پیام زیر نمایش داده شود.

()	Ø https://mydomain.com/ ♀ < ♂ × Ø Certificate Error: Navigation ×
8	There is a problem with this website's security certificate.
	The security certificate presented by this website was issued for a different website's address.
	Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.
	We recommend that you close this webpage and do not continue to this website.
	Ø Click here to close this webpage.
	Sontinue to this website (not recommended).
	More information

دلیل مشکل فوق این است که آدرس سایت را بطور دقیق وارد ننمودهاید. در زیر، چند سناریو که منجر به چنین خطایی می شوند آورده شده است:

اگر گواهی برای www.mydomain.com صادر شده باشد اما آدرس https://mydomain.com
 اگر گواهی برای را در مرورگر وارد نمایید، با صفحه خطای فوق مواجه می شوید. برای رفع این
 مشکل، یا باید همیشه آدرس دقیق وارد شود یا راه حل بهتر اینکه در تنظیمات سرور خود، آدرس

https://mydomain.com را به https://www.mydomain.com (یعنی با آدرس دقیق) تغییر مسیر دهید (redirect نمایید).

- ممکن است یک سایت، به چند دامنه (مثلاً mydomain.com و mydomaint.ir) تخصیص داده شده باشد. مثلاً اگر گواهی سایت برای www.mydomain.com صادر شده باشد اما آدرس https://www.mydomain.ir
 می شوید. در صورتی که برای یک سایت چند دامنه وجود داشته باشد اما گواهی شما فقط برای یک دامنه صادر شده باشد، باید از مرکز صدور گواهی درخواست گواهی SAN نمایید. کاربرد گواهی RAN برای استفاده از یک گواهی برای چندین دامنه است.
- ممکن است برای یک سایت فقط یک دامنه وجود داشته باشد اما در آن دامنه، زیردامنه' نیز وجود داشته باشد (مثلاً mail.mydomain.com). حال اگر آدرس https://mail.mydomain.ir را در مرورگر وارد نمایید، با صفحه خطا مواجه می شوید. در صورتی که بخواهید برای زیردامنه خود نیز از HTTPS استفاده نمایید، باید یک گواهی مجزا برای این زیر دامنه درخواست نمایید. در صورتی که بخواهید فقط از یک گواهی برای یک دامنه و تمام زیردامنههایش استفاده کنید، می توانید درخواست گواهی لیاید.

توجه: ممکن است صفحههای هشدار مشابه دیگری با دلایل خاص خود وجود داشته باشد که معمولاً مربوط به پیکربندی سرور شما میباشد. در صورت مواجهه با چنین خطاهایی، آنها را به دقت مطالعه نموده و با انجام تنظیمات لازم روی سرور، آنها رفع نمایید.

۷-۳ نمایش صفحه دیگری به جای صفحه سایت

برای استفاده از HTTPS برای یک دامنه (وبسایت)، باید یک آدرس IP اختصاصی (Dedicated IP Address) به آن دامنه تخصیص داده شود (رویه تخصیص IP اختصاصی در بخش ۵–۲ توضیح داده شده است). در صورتی که آدرس IP سایت با سایتهای دیگر به اشتراک گذاشته شده باشد (یرا Shared) باشد)، هنگام درخواست HTTPS، سرور معمولاً صفحه پیشفرض IIS را نشان میدهد (زیرا نمی تواند تشخیص دهد چه سایتی را برگرداند).

¹ Subdomain

© Copyright Amnafzar Co.

۴–۷ نمایش صحیح سایت HTTPS در یک مرورگر و عدم نمایش آن در مرورگری دیگر

این مشکل مربوط به گواهی SSL سایت نیست، زیرا گواهی صادرشده توسط مرکز میانی پارسساین از استانداردی (استاندارد X.509) تبعیت میکند که وابسته به مرورگر یا سیستمعامل خاصی نیست. این مشکل معمولاً به دلیل استفاده از مرورگر یا سروری است که بروزرسانی نشده است. در صورتی که مرورگر و سرور هر دو به روز باشد، مشکل در تنظیمات SSL سرور است. علاوه بر بحث بروز رسانی، در برخی مرورگرها ممکن است تنظیمات SSL صحیح نباشد، لذا از این موضوع نیز اطمینان حاصل نمایید.

۸ پيوست

N=A نحوه بررسی PEM بودن فایل کلید و تبدیل آن به فرمت PEM

برای بررسی PEM بودن فرمت فایل کلید خصوصی، آن را با یک ویرایشگر متن باز مینماییم. به طور مثال در ویندوز، روی فایل راستکلیک مینماییم و گزینه Open with، سپس Popram را انتخاب را انتخاب کرده و در بخش Other Programs از صفحه ظاهرشده، نرم افزار WordPad را انتخاب مینماییم.) در صورتی که فایل با عبارتی مشابه -----BEGIN RSA PRIVATE KEY می باشد. به -----BEGIN RSA PRIVATE KEY می باشد، فرمت فایل از نوع PEM می باشد.

نکته: در صورتی که CSR با نرمافزار ParsKey Utility تولید شده باشد، فایل کلید در فرمت PEM می باشد.

اگر کلید خصوصی به فرمت PEM نباشد (مثلاً در فرمت DER باشد)، باید مراحل زیر را برای تبدیل آن از فرمت DER به فرمت PEM انجام دهیم:

- به وبسایت مرکز صدور گواهی الکترونیکی پارسساین به آدرس <u>www.parssignca.ir</u> مراجعه نموده و نرمافزار OpenSSL را از بخش دانلود سایت دریافت نموده و روی سیستم خود نصب می نماییم.
- ۲. اگر نسخهی تحت ویندوز OpenSSL را نصب کرده باشیم، به دایرکتوری bin در مسیر نصب نرمافزار رفته (این مسیر در ویندوز 7 نسخه ۶۴ بیتی، C:\OpenSSL-Win64\bin میباشد) و فایل اجرایی OpenSSL به نام openssl.exe را اجرا مینماییم. با اجرای این برنامه، پنجرهای مانند شکل زیر ظاهر



۳. روبروی عبارت <OpenSSL در پنجره فوق، دستور زیر را وارد مینماییم:

rsa -inform der -in key.der -outform pem -out key.pem

لازم به ذکر است که اگر با لینوکس کار میکنیم، دستور زیر را وارد مینماییم:

openssl rsa -inform der -in key.der -outform pem -out key.pem

لازم به ذکر است که برای هر یک از فایلهای فوق، باید مسیر دقیق آنها را در دستور وارد نماییم. برای مثال، در صورتی که فایل key.der را در درایو D و پوشه keys قرار داده باشیم و میخواهیم فایل key.pem نیز در همین مسیر ذخیره گردد، دستور به صورت زیر خواهد بود:

rsa -inform der -in d:\keys\key.der -outform pem -out d:\keys\key.pem

در صورت استفاده از لینوکس، فرض میکنیم فایل های مذکور در مسیر home/keys/ قرار داشته باشند. به این ترتیب، دستور زیر را وارد مینماییم:

openssl rsa -inform der -in /home/keys/key.der -outform pem -out /home/keys/key.pem

۸–۲ نحوه بررسی PEM بودن فرمت فایل گواهی و تبدیل آن به فرمت PEM

برای بررسی PEM بودن فرمت فایل گواهی، آن را با یک ویرایشگر متن باز مینماییم. به طور مثال در ویندوز، روی فایل راستکلیک مینماییم و گزینه Open with، سپس Choose default program را انتخاب کرده و در بخش Other Programs از پنجره ظاهرشده، نرمافزار WordPad را انتخاب مینماییم. در صورتی که فایل با عبارت ----- BEGIN CERTIFICATE----- شروع و به ----- END CERTIFICATE میباشد.

اگر فرمت فایل pem نباشد، آن را به صورت زیر به یک فایل گواهی جدید با فرمت PEM تبدیل مینماییم:

- ۱. ابتدا فایل مورد نظر را باز مینماییم. برای این کار، روی فایل گواهی دابل کلیک نموده، سپس در پنجره ظاهرشده روی دکمه Open کلیک مینماییم.
 - ۲. در پنجره بازشده، در سربرگ Details روی دکمه Copy to Files کلیک می نماییم (مانند شکل زیر).

Certificate	h	x
Show: <all></all>	~	
Field	Value	
Version	V3	
Serial number	22	=
📴 Signature algorithm	sha 1RSA	
🔄 Signature hash algorithm	sha 1	
📴 Issuer	root_self_signed_test, pki, am	
Valid from	Sunday, October 21, 2012 10:	
🔲 Valid to	Saturday, August 17, 2013 10	
Subject	www.v3demoh.cnv3demo.co	Ŧ
	2	
E Learn more about <u>certificate detail</u>	Edit Properties Copy to File) K

۳. در پنجره Certificate Export Wizard روی Next کلیک می نماییم (مانند شکل زیر).



۶. در پنجره Export File Format در بخش Select the format you want to use گزینه (مانند شکل Next) کلیک می کنیم (مانند شکل Next) (CER) را انتخاب نموده، سپس روی Next کلیک می کنیم (مانند شکل زیر).

ertificate Export Wizard				
Export File Format Certificates can be exported in a variety of file formats.				
Select the format you want to use: O DER encoded binary X.509 (.CER)				
Base-64 encoded X.509 (.CER)				
Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B) Include all certificates in the certification path if possible				
 Personal Information Exchange - PKCS #12 (.PFX) Include all certificates in the certification path if possible 				
Delete the private key if the export is successful				
Export all extended properties				
Microsoft Serialized Certificate Store (.SST)				
Learn more about <u>certificate file formats</u>				
< Back Next > Cancel				

۵. در پنجره File to Export برای انتخاب مسیر ذخیره فایل با فرمت pem، روی Browse کلیک مینماییم. پس از انتخاب نام و مسیر ذخیره فایل، روی Next کلیک مینماییم (مانند شکل زیر).

File to Export	
Specify the name of the file you want to e	xport
	1
File name:	
E:\website_pem_cert.cer	Browse
	2

۶. در پنجره Completing the Certificate Export Wizard روی Finish کلیک مینماییم (مانند شکل



۷. پنجره زیر که نشاندهنده موفق بودن تبدیل فایل میباشد، ظاهر می گردد. روی OK کلیک مینماییم. به
 این ترتیب، عملیات تبدیل فایل به فرمت pem پایان می پذیرد.

Certificate Export Wizard
The export was successful.
ОК